系列のLinear Complexityの拡張とその応用(数理モデルの組合せ論的構造)

AUTHOR(S):

上原, 聡; 森内, 勉; 今村, 恭己

数理解析研究所講究録
第853巻 1993年 31-40

系列のLinear Complexityの拡張とその応用

九工大・情報工　上原　聡　(Satoshi Uehara)
八代高専　森内　勉　(Tsutomu Moriuchi)
九工大・情報工　今村　恭己　(Kyoki Imamura)

1 まえがき

系列のComplexity(予想し難さ、解読し難さ)に対する評価尺度の中でも特にLinear Complexity (LC)は、Berlekamp-Masseyアルゴリズムを初めとしてEuclidの互除法を用いる方法や連分数を用いる方法など数多くの高速アルゴリズムがあることからこれまで広く用いられている。しかしながら、Linear Complexityに問題点が無いわけではない。本稿で取り上げる系列に対するLCの評価は非常に高いものであるが、系列の構成法から見て過大評価に思われる。

有限体$GF(q^n)$の原始元をα、$GF(q^n)$から$GF(q)$へのトレース: $tr()$を

$$tr(\beta)=\sum_{i=0}^{n-1}\beta^{q^i}, \qquad \beta\in GF(q^n)$$

としたとき、周期$T=q^n-1$の$GF(q)$上のm-系列$\{m_i\}$:

$$m_i=tr(\alpha^i) \tag{1}$$

の最小変更によって得られる系列$\{a_i\}$を

$$a_i=\begin{cases} m_j+b,\ (b\in GF(q)\backslash\{0\}) & \text{if } i=j \pmod T,\\ m_i & \text{otherwise.}\end{cases} \tag{2}$$

とする[1]。つまり、この系列はm-系列の1周期中の1シンボルの変更によって構成されたものである。そこで、定数:$b=\alpha^{uT/(q-1)}$, $0\le u\le q-2$としてこの系列$\{a_i\}$に対するLCの値を求めると、次のような2値を取ることが分かった[1, 2]。

$$LC=\begin{cases} T & \text{if } j\neq uT/(q-2),\\ T-n & \text{otherwise.}\end{cases} \tag{3}$$

しかし、この結果はm-系列のLCがnであることを考えるとあまりにも大き過ぎる値となっている。

LCと同様にFeedback Shift Register (FSR)の段数によって評価するComplexityがある。それらはQuadratic Complexity (QC)[3], Maximum Order Complexity (MOC)[4]と呼ばれるもので、どれも評価対象となる系列を生成することのできるFSRの最小段数として与えられる。異なる点はFeedback関数の次数にあり、表1に示す通りである。したがって、同じ系列に対するそれぞれのComplexityの評価は

$$MOC\le QC\le LC$$

表 1: Feedback 関数の次数と Complexity との関係

Complexity	Feedback 関数の次数
Linear Complexity (LC)	1
Quadratic Complexity (QC)	2
Maximum Order Complexity (MOC)	無制限

表 2: m- 系列の最小変更によって得られる系列の Complexity

Complexity	LC^*	QC^{**}	MOC^{***}
最大値	T	$T-\binom{n+1}{2}$	$2n$
最小値	$T-n$	$n+1$	n

* LC は 2 値しか取らず、ある条件を満足したときに $LC = T-n$ となる。

** QC の最大値・最小値は、数値実験からの予想である。

*** $(q,n) = (2,2)$ の場合には、$2n, n$ を、それぞれ $2(=n), 1(=T-n)$ で置き換える。

となる。さらに、周期 T, $GF(q)$ 上の系列に対する Complexity についてはその定義から次の関係が成り立つ。

$$\lceil \log_q T \rceil \leq MOC \leq QC \leq LC \leq T \tag{4}$$

これら 3 つの Complexity を使って系列 $\{a_i\}$ の評価を行なった結果を表 2に示す。これより、m- 系列の LC が n であるのに対して最も理に適った結果が得られたのは、MOC の場合の $n \leq MOC(\{a_i\}) \leq 2n$ であることが分かった。

本稿では、m- 系列の最小変更によって得られる系列の評価と言う点で最も適当な結果が得られた MOC の範囲 $(n \leq MOC(\{a_i\}) \leq 2n)$ についての証明を行い、さらに MOC が n や $2n$ となる場合や $MOC = 2n$ となる系列 $\{a_i\}$ の構成例を示す。

2 系列 $\{a_i\}$ の MOC

Maximum Order Complexity は、論文 [4] の中で次のように定義されている。

定義 1 ある系列を *Feedback Shift Register (FSR)* と *Feedback Function* F とからなる図 *1*の回路で生成するとき、その *FSR* の段数 n の最小値をその系列の *Maximum Order Complexity (MOC)* とする。

図 1の回路において $F()$ は $s_0, s_1, \ldots, s_{n-1}$ の一価関数であることから、系列 $\{s_i\}$ の MOC を c とすると $F(s_i, s_{i+1}, \ldots, s_{i+n-1}) = s_{i+n}$ の関係がすべての $i \geq 0$ について成り

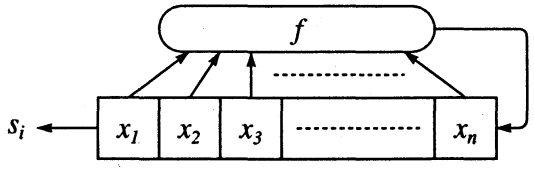


図 1: The feedback shift register.

立つ最小の n が c となる [4]。これは言い換えると、$\{s_i\}$ において $(s_i, s_{i+1}, \ldots, s_{i+n-2}) = (s_j, s_{j+1}, \ldots, s_{j+n-2})$ $(i \neq j)$ かつ $s_{i+n-1} \neq s_{j+n-1}$ となるような i, j $(i \neq j)$ が存在する中で最も大きな n が c であることを意味している。したがって周期 T の周期系列 $\{s_i\}$ についての MOC は、k を 1 から $T-1$ まで動かしたときの系列 $\{s_i - s_{i+k}\}$ の 1 周期 $(0 \leq i \leq T-1)$ 中に出現する '0' の連の長さの最大値が $c-1$ であることを利用して容易に計算することができる。

特に m- 系列 $\{m_i\}$ の場合には、次式で示される通り減算した系列も同じ m- 系列となることはよく知られた性質である。

$$\begin{aligned} m_i - m_{i+k} &= tr(\alpha^i) - tr(\alpha^{i+k}) \\ &= tr(\alpha^i(1-\alpha^k)) \\ &= tr(\alpha^i \alpha^{\mathcal{Z}(k)}) \\ &= m_{i+\mathcal{Z}(k)} \end{aligned} \tag{5}$$

ただし、$\mathcal{Z}(k)$ は $\alpha^{\mathcal{Z}(k)} = 1 - \alpha^k$ で定義される関数である。したがって、m- 系列が最大長 $n-1$ の '0' の連を持つことから、m- 系列の MOC は n であることがわかる。

さらに、m- 系列 $\{m_i\}$ の最小変更によって得られる系列 $\{a_i\}$ の範囲に関して次の定理が成り立つ。

定 理 1 周期 $T = q^n - 1$ の m- 系列 $\{m_i\}$ の最小変更によって得られる系列 $\{a_i\}$ の MOC $(= c)$ は、$(q,n) = (2,2)$ の場合を除くと

$$n \leq c \leq 2n$$

を満足する。なお、$(q,n) = (2,2)$ の場合は、$c = 1(= T-n)$ または $c = 2(= n)$ である。

証 明 : $(q,n) = (2,2)$ の場合は、$\{m_0, m_1, m_2\} = \{0,1,1\}$, $\{a_0, a_1, a_2\} = \{1,1,1\}$ or $\{0,0,1\}$ or $\{0,1,0\}$ であるので、$c = 1(= T-n)$ または $c = 2(= n)$ である。したがって、以下では $(q,n) \neq (2,2)$ の場合について考える。

まず $c \geq n$ であることを示す。$\{a_i\}$ の周期を T' とすると、$a_{i+T} = a_i$ が任意の $i \geq 0$ について成り立つので、

$$T = kT' \qquad (k : \text{正整数}) \tag{6}$$

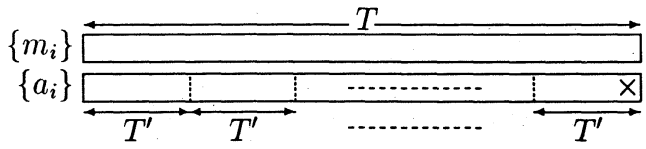


図 2: An image of the sequence $\{a_i\}$.

となる。ここで、$T = T'$、つまり $k = 1$ ならば、

$$T' \leq q^c \tag{7}$$

により $q^c \geq q^n - 1$ であるので、

$$c \geq n \tag{8}$$

が成り立つ。

そこで、

$$c < n \tag{9}$$

と仮定すると、(6), (7) により、

$$qT' \leq q^n = T + 1 = kT' + 1$$

であるので、

$$(q - k)T' \leq 1 \tag{10}$$

を得る。q, k, T' は正整数であるので、(10) より

$$k \geq q \tag{11}$$

である。さらに $q = 2$ の場合には $T = q^n - 1$ が奇数であることから、(6) において $k \neq 2$ であるので、(11) は、

$$k \geq max(q,\ 3) \geq 3 \tag{12}$$

と書ける。また $\{m_i\}$ の周期 T と $\{a_i\}$ の周期 T' の間の関係と $\{a_i\}$ の MOC とを調べるためには、

$$\left.\begin{array}{lll} a_i = m_i & \text{if} & i \not\equiv T - 1 \pmod{T}, \\ a_i \neq m_i & \text{if} & i \equiv T - 1 \pmod{T}. \end{array}\right\} \tag{13}$$

の場合のみを考えても、一般性を失わない (図 2)。ところで (6), (12) から $T \geq T' + \frac{2}{3}T$ であるので、$n \geq 2$ かつ $(q, n) \neq (2, 2)$ に対して $2(q^n - 1) > 3n$ であることを考慮すると、

$$T - 1 \geq T' + \frac{2}{3}(q^n - 1) - 1 > T' + n - 1 \tag{14}$$

となる。したがって、

$$a_i = a_{i+T'} \tag{15}$$

と、(14) とにより、

$$m_i = m_{i+T'} \qquad (0 \le i \le n-1,\ T'+n-1 < T-1) \tag{16}$$

が成り立つ。(16) は、m- 系列の 1 周期中に同じ n-tuple が 2 回以上出現することを意味しているが、このようなことは m- 系列 $\{m_i\}$ ではあり得ない。したがって、(9) を仮定すると元の $\{m_i\}$ が m- 系列であることに矛盾することから (8) が証明されたことになる。

次に、$c \le 2n$ であることを示す。(2), (5) により

$$a_i - a_{i+k} = \begin{cases} m_{i+\mathcal{Z}(k)} + b & \text{if } i \equiv j \pmod T, \\ m_{i+\mathcal{Z}(k)} - b & \text{if } i \equiv j-k \pmod T, \\ m_{i+\mathcal{Z}(k)} & \text{otherwise.} \end{cases} \tag{17}$$

となる (ただし、$\alpha^{\mathcal{Z}(k)} = 1 - \alpha^k$)。$k$ $(1 \le k \le T-1)$ を適当に選ぶと、系列 $\{a_i - a_{i+k}\}$ の 1 周期中 $(0 \le i \le T-1)$ には、長さ $c-1$ の '0' の連が出現する。いま k をそのように選び、長さ $c-1$ の '0' の連が $i = i_0$ から $i = i_0 + c - 2$ の間で出現したとする。系列 $\{m_{i+\mathcal{Z}(k)}\}$ は元の m- 系列を位相 $\mathcal{Z}(k)$ だけシフトしたものであるので、'0' の連の長さは $n-1$ 以下であり、長さ $n-1$ の '0' の連は丁度 1 個である。もしも

$$i_0 < j, \quad j-k \pmod T < i_0 + c - 2 \tag{18}$$

でないならば、(17) により $c - 1 \le (n-1) + (n-2) + 1 = 2n - 2$ となる。したがって $c > 2n$ となるとすれば、(18) が成り立ち、$\{m_{i+\mathcal{Z}(k)}\}$ は、

$$\{m_{i+\mathcal{Z}(k)}\} = \cdots \delta_0 \underbrace{\underbrace{0\cdots\cdots0}_{d_1} - b \underbrace{0\cdots\cdots0}_{d_2} + b \underbrace{0\cdots\cdots0}_{d_3}}_{c-1=d_1+d_2+d_3+2} \delta_3 \cdots \tag{19}$$

$$\delta_0 \neq 0,\ \delta_3 \neq 0$$

と書ける。以下では、$c > 2n$ を仮定すると元の系列 $\{m_{i+\mathcal{Z}(k)}\}$ は m- 系列ではあり得ないことを示すことにより $c \le 2n$ を証明する。

系列 $\{a_i\}$ が $2n$ を越える MOC を持つ、すなわち

$$c > 2n \tag{20}$$

と仮定し、元の m- 系列 $\{m_l\} = \{m_{i+\mathcal{Z}(k)}\}$ について考察する。

m- 系列 $\{m_l\}$ は、

$$m_l = \sum_{i=0}^{n-1} \sigma_i m_{l-n+i} \tag{21}$$

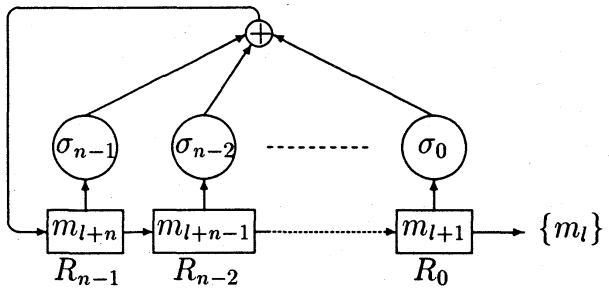


図 3: A linear feedback shift register for generating $\{m_l\}$.

により生成されるとする。これから $n \times n$ Hankel 行列 $[m_{i,j}]$ を係数行列とする $\sigma_0 \sim \sigma_{n-1}$ に関する方程式が得られる。

$$\begin{bmatrix} m_l & m_{l+1} & m_{l+2} & \cdots & m_{l+n-1} \\ m_{l+1} & m_{l+2} & \cdots\cdots & & m_{l+n} \\ m_{l+2} & & & & \vdots \\ \vdots & & & & \vdots \\ m_{l+n-1} & \cdots\cdots & & & m_{l+2n-2} \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \vdots \\ \sigma_{n-1} \end{bmatrix} = \begin{bmatrix} m_{l+n} \\ m_{l+n+1} \\ \vdots \\ \vdots \\ m_{l+2n-1} \end{bmatrix} \tag{22}$$

したがって、m_l を式 (19) において δ_0 の次に続く '0' とすると、(22) は、

$$\overset{d_1+1\Rightarrow}{} \begin{bmatrix} 0 & \overset{d_1+1}{\Downarrow} & \\ & -b & \\ -b & 0 & b \\ & b & \\ & \underset{d_1+d_2+3-n}{\Uparrow} & 0 \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \vdots \\ \sigma_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ b \\ 0 \\ \vdots \\ 0 \end{bmatrix} \overset{\Leftarrow d_1+d_2+2-n}{} \tag{23}$$

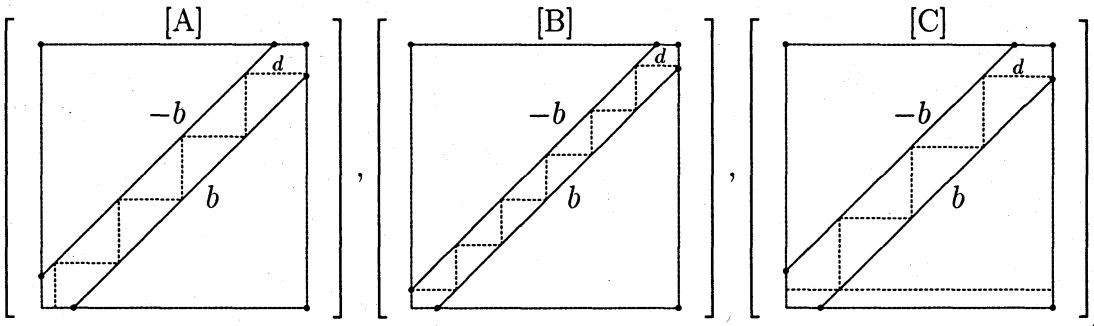
$$1 \le d_1 \le n-1$$

$$1 \le d_1 + d_2 + 2 - n \le n-1$$

と書き換えることができる。ただし、左辺の係数行列の要素は斜線部 $-b$, b 以外すべて '0' となる。

しかし、m-系列の持つ性質よりもっとも長い '0' の連の長さは $n-1$ であり、一周期の中に一度だけ現れる。したがって、$d_1 + 1 \le n$, $d_1 + d_2 + 3 - n \le n$, $(d_1 + 1) - (d_1 + d_2 + 3 - n) \ge -1$ であるので、(23) の左辺の Hankel 行列は、次の三つに限定され

る $(d = d_2 + 1)$。



(24)

まずタイプ [C] の場合は、方程式の形から $\sigma_{n-d} = -1$ かつ $\sigma_{n-d} = 0$ となり矛盾する。

次にタイプ [A] の場合は方程式の形から元の m- 系列 $\{m_l\}$ の特性多項式

$$f(x) = x^n - \sum_{i=0}^{n-1} \sigma_i x^i \tag{25}$$

は $n = rd + n_0\ (0 < n_0 < d)$ として、

$$f(x) = (x^{rd} + x^{(r-1)d} + \cdots + x^d + 1)(x^{n_0} + a_{n_0-1}x^{n_0-1} + \cdots + a_0) \tag{26}$$

と書ける。したがって $f(x)$ が原始多項式ではないので矛盾する。

最後に [B] の場合には、$n = rd\ (r \geq 1)$ であって、

$$\begin{aligned} f(x) &= x^{rd} + x^{(r-1)d} + \cdots + +x^d + 1 \\ &= \begin{cases} \dfrac{x^{(r+1)d} - 1}{x^d - 1} & \text{if } r \geq 2, \\ x^n + 1 & \text{if } r = 1. \end{cases} \end{aligned} \tag{27}$$

となる。系列 $\{m_l\}$ が m- 系列であるためには、$f(x)$ の根 α は $GF(q^n)$ の原始元でなければならない。すなわち、

$$\alpha^{q^{rd}-1} = 1, \qquad \alpha^i \neq 1 \quad \text{for } 1 \leq i \leq q^{rd} - 2 \tag{28}$$

が成り立たねばならない。なお、$GF(q^n)$ の標数 p が $p = 2$ の場合には、$x + 1 \mid x^n + 1$ であるので、(27) において $r = 1$ の場合は除外される。また $r = 1$ の場合は、$d = n$ であるので、(27) は $r = 1$ の場合も含めて

$$f(x) = \frac{x^{(r+1)d} - 1}{x^d - 1} \qquad (r \geq 1) \tag{29}$$

と書ける。ただし $p = 2$ の場合は、$r \geq 2$ である。式 (29) から

$$\alpha^{(r+1)d} = 1 \tag{30}$$

となる。付録で証明するように、$(q, r) = (2, 1)$ の場合を除くと $d \geq 2$ に対して、

$$q^{rd} - 1 > (r + 1)d \tag{31}$$

であるので、(30) は (28) に矛盾する。以上の議論により、(19) のようなパターンは存在しないことになり、$c \leq 2n$ であることが分かった。したがって $(q,n) \neq (2,2)$ ならば

$$n \leq c \leq 2n \tag{32}$$

である。 **Q.E.D.**

以下、$c = n$, $c = 2n$ となる場合の例を示す。

元の m- 系列 $\{m_i\}$ の生成多項式を次式とする。

$$f(x) = x^n \mp dx \pm d \quad (d \in GF(q) \setminus \{0\})) \tag{33}$$

このとき m- 系列の性質より、一周期中の n-tuple を見ると all-'0' 以外のすべてのパターンが存在することから、m- 系列には次のようなパターンが必ず存在することになる。

$$(e, e, \ldots, e) \quad (e \in GF(q) \setminus \{0\}))$$

この系列の続きは、このときの生成多項式 (33) により

$$\cdots, \underbrace{e, e, \ldots, e}_{n}, \underbrace{0, 0, \ldots, 0}_{n-1}, \mp de, \cdots$$

となる。したがって、長さ $n-1$ の '0' の連に隣接する長さ n の 'e' の連の最後のシンボルに $b = -e$ を加えて系列 (2) を作ることで、この系列の一周期中に現れる長さ n の tuple を見ると all-'e' を除くすべてのパターンが必ず一度現れることが分かる。MOC が c となる時に最大長の系列となるのは、一周期中に長さ $n = c$ のすべてのパターンが一度のみ現れる場合だけであることから、今考えている系列において all-'e' だけが出現しないことを考えるとこの系列の MOC は $c \leq n$ の範囲に限られる。さらに定理 1 より $c \geq n$ となることが証明されたことから、この系列の MOC は $c = n$ となる。

次に系列の MOC が $c = 2n$ となる例として、元の m- 系列 $\{m_i\}$ の生成多項式が

$$f(x) = x^n + x^l + \frac{\delta_3}{b} \quad (b, \delta_3 \in GF(q) \setminus \{0\}) \tag{34}$$

となる場合について考察する。m- 系列の性質より、一周期中の n-tuple を見ると all-'0' 以外のすべてのパターンが存在することから、m- 系列には次のようなパターンが必ず存在することになる。

$$(0, 0, \ldots, 0, \mp b)$$

したがって、(34) で示される生成多項式により系列 (19) を生成することができる。このとき

$$\begin{aligned} d_1 &= n-1 \\ d_2 &= n-l-1 \\ d_3 &= l-1 \end{aligned} \tag{35}$$

と書けることから、

$$c-1=d_1+d_2+d_3+2=2n-1$$

となる。つまり (34) を生成多項式とする m- 系列の最小変更によって得られる系列の MOC は $c=2n$ であることを示している。なお、(33) または (34) の形の 3 項原始多項式が実際に存在することは、$q=2$ の場合には多数の n について知られている。

さらに、元の m- 系列 $\{m_i\}$ の生成多項式を次のように限定することで、$MOC=2n$ となる場合の最小変更によって得られる系列 $\{a_i\}$ を構成することができる。3 項の生成多項式:

$$f(x)=x^n+x+1$$

により、次のような m- 系列を生成することができる。

$$\{m_i\}=\cdots\underbrace{1\cdots1}_{n}\underbrace{0\cdots0}_{n-1}1\underbrace{0\cdots0}_{n-2}11\underbrace{0\cdots0}_{n-3}101\cdots$$

したがって、n が偶数の場合には $tr(\alpha^{n-2})$、n が奇数の場合には $tr(\alpha^{n-1})$ の '0' を '1' とすることで、

$$\{m_i\}=\cdots\underbrace{1\cdots1}_{n}\underbrace{0\cdots\overset{1}{\not0}}_{n-1}1\underbrace{0\cdots0}_{n-2}11\underbrace{0\cdots0}_{n-3}101\cdots$$

$$\{m_i\}=\cdots111\overbrace{\underbrace{0\cdots0}_{n-2}11\underbrace{0\cdots00}_{n-2}11\underbrace{0\cdots0}_{n-3}}^{2n-1}101\cdots$$

長さ $2n-1$ の同じパターンが 1 周期中に現れることになり、$MOC=2n$ となる系列を得ることができる。また、同じ系列中の '1' を '0' と変更することで同じように $MOC=2n$ となる。その変更点は、n が偶数の場合で $tr(\alpha^{2n-1})$、奇数の場合で $tr(\alpha^{2n})$ を変更すればよい。

$$\{m_i\}=\cdots\underbrace{1\cdots1}_{n}\underbrace{0\cdots0}_{n-1}1\underbrace{0\cdots0}_{n-2}1\overset{0}{\not1}\underbrace{0\cdots0}_{n-3}101\cdots$$

$$\{m_i\}=\cdots\overbrace{\underbrace{00\cdots0}_{n-1}1\underbrace{0\cdots0}_{n-2}1\underbrace{00\cdots0}_{n-2}}^{2n-1}101\cdots$$

3 まとめ

本稿では、m- 系列 $\{m_i\}$ の最小変更によって得られる系列 $\{a_i\}$ に対する Complexity の結果が最も適当だと思われる MOC について、その範囲が $n\leq c\leq 2n$ となることを証明した。さらに、MOC が最大の値を取る場合についても構成例を挙げて示している。今回 m- 系列の最小変更によって得られる系列の Complexity 評価は、MOC が最もよい結果を示しているが、他の系列に対しては、別の Complexity で十分となる可能性は大きい。したがって、今後、他の系列に対する Complexity を計算することで、一般的に LC, QC, MOC の評価を行う必要がある。

参考文献

[1] K. Imamura T. Moriuchi and S. Uehara, "Periodic sequences of the maximum linear complexity simply obtained from an m-sequence", *Proc. IEEE 1991 Intern. Symp. Inform. Theory*, p.175, June 1991.

[2] 今村 恭己, "系列の Linear Complexity", 数理解析研究所講究録 820, pp. 59-71, 1993.

[3] A. H. Chan and R. A. Games, "On the Quadratic Spans of DeBruijn Sequences", IEEE Trans. Inform. Theory, vol. 36, No. 3, pp. 822-829, 1990.

[4] C. J. A. Jansen and D. E. Boekee, "The shortest feedback shift register that can generate a given sequence", *Proc. CRYPT '89 (Lecture Note in Computer Science, vol. 435)*, pp.90-99, Springer-Verlag, 1990.

付 録 式 (31) の証明：$d = d_2 + 1 \geq 2$ により、

$$\begin{aligned} q^{rd} - 1 &= [1 + (q-1)]^{rd} - 1 \\ &\geq rd(q-1) + \frac{rd(rd-1)}{2}(q-1)^2 \end{aligned} \tag{A1}$$

$q = 2$ の場合には、$r \geq 2$ により、(A1) は

$$q^{rd} - 1 \geq rd + d(rd-1) \geq rd + 3d > (r+1)d$$

となる。$q > 2$ の場合には、(A1) は

$$q^{rd} - 1 > rd + rd(rd-1) \geq rd + d = (r+1)d$$

となる。 **Q.E.D.**